

Curs 6 - 11.11.2024

Struct Algebraic in Informatică

Dacă $M_n = 2^n - 1$ este prim $\Rightarrow n$ este
prim ~~este~~

Aritmetică modulară

înmulțirea \mathbb{Z}_m

Fixăm $2 \leq m \in \mathbb{N}$. Definim pe \mathbb{Z} relația de
~~convergență~~ congruență modulo m .

$$x \equiv y \pmod{m} \Leftrightarrow m|x-y$$

sau

$$\text{notat } x \stackrel{(m)}{\equiv} y$$

Prop: $\equiv \pmod{m}$ este o relație de echivalență.
 $\forall x, y \in \mathbb{Z} : x \equiv y \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z} : x = y + km$

Prop: $x \equiv y \pmod{m} \Leftrightarrow x, y$ au același
rest la împărțirea la m .

Prop. Dem: Scriem $x = q_1 m + r_1$ cu $q_1, r_1 \in \mathbb{Z}$,
 $y = q_2 m + r_2$ cu $q_2, r_2 \in \mathbb{Z}$,
 $0 \leq r_1, r_2 < m$

$$x - y = m(q_1 - q_2) + r_1 - r_2 \quad -m < r_1 - r_2 < r_1, \quad r_1, r_2 \leq m$$

$$x - y \equiv r_1 - r_2 \pmod{m} \quad r_1, r_2 \leq m \quad (\star)$$

$$\downarrow \quad (\star) \quad r_1 = r_2$$

$$x \equiv y \pmod{m} \quad r_1 = r_2$$

Proprietăți: Fix $a, x, y \in \mathbb{Z}$. Dacă $x \equiv y \pmod{m}$

$$\Rightarrow x+a \equiv y+a \pmod{m}$$

$$ax \equiv ay \pmod{m}$$

Azm: Iată $n | x-y = (x+a) - (y+a) \Rightarrow$

$$\Rightarrow x+a \equiv y+a \pmod{n}$$

$$n | a(x-y) = ax - ay \Rightarrow ax \equiv ay \pmod{n}$$

Spre deosebită se notează că $\mathbb{Z}_m = \{x^{\wedge} \mid x \in \mathbb{Z}\}$

$\{0^{\wedge}, 1^{\wedge}, \dots, m-1^{\wedge}\}$ este sistem de reprezentanțe

$$x^{\wedge} \equiv \pmod{m} \Rightarrow \mathbb{Z}_m = \{0^{\wedge}, 1^{\wedge}, \dots, m-1^{\wedge}\}$$

Teorema: \mathbb{Z}_m cu operațiile de „+” și „ \cdot ” definite:

$$x^{\wedge} + y^{\wedge} = x^{\wedge} \widehat{+} y^{\wedge}, \quad \forall x, y \in \mathbb{Z}_m \text{ este un inel comutativ}$$

$$x^{\wedge} \cdot y^{\wedge} = x^{\wedge} \widehat{\cdot} y^{\wedge}$$

• 0^{\wedge} este elem. neutru la „+”

• opusul lui x^{\wedge} este $-x^{\wedge} = \widehat{-x}$

• 1^{\wedge} este elem. neutru la înmulțire

$$x^{\wedge} \cdot y^{\wedge} = x^{\wedge} \widehat{\cdot} y^{\wedge} = y^{\wedge} \cdot x^{\wedge}$$

obs! Operațiile definite pe \mathbb{Z}_m nu depind de reprezentanții lor

$$\text{Ei } x = x_1^{\wedge} \text{ și } y = y_1^{\wedge} \Rightarrow n | x - x_1^{\wedge} \quad \stackrel{\oplus}{\iff} \quad n | y - y_1^{\wedge}$$

$$n | (x - x_1^{\wedge}) + (y - y_1^{\wedge}) \quad \Rightarrow \quad x^{\wedge} \widehat{+} y^{\wedge} = x_1^{\wedge} \widehat{+} y_1^{\wedge}$$

$$x \cdot y - x_1 \cdot y_1 = x(y - y_1) + x y_1 - x_1 y_1 = x(y - y_1) +$$

$$+ y_1(x - x_1) : m \Rightarrow \widehat{xy} = \widehat{x_1 y_1}$$

$x \in \mathbb{Z}_m$ este inversabilă dacă și " "

dacă $\exists y \in \mathbb{Z}_m$ a.s. $x \cdot y = y \cdot x = 1 \Leftrightarrow xy = 1$

$\Leftrightarrow m \mid 1 - xy \Leftrightarrow \exists u \in \mathbb{Z}$ a.s. $1 - xy = u \cdot m$

$x \in \mathbb{Z}_m$ inversabil $\Leftrightarrow \exists y, u \in \mathbb{Z}$ a.s.

 $xy + u \cdot m = 1 \Leftrightarrow \gcd(x, m) = 1$

$$0 \leq x \leq m-1$$

Prop: $|U(\mathbb{Z}_m)| = \{x \in \mathbb{Z}_m \mid \gcd(x, m) = 1\}$

Functia indicatoare a lui Euler

$\ell(m) := m$ de intregi între $1, m-1$ primi cu

$$m | U(\mathbb{Z}_m) | = \ell(m)$$

Pornind că do obiecte parcurguri în m în
factori primi: $m = p_1^{d_1} \cdot p_2^{d_2} \cdots p_t^{d_t}$ ca

p_1, p_2, \dots, p_t , prime distincte

$$d_1, \dots, d_t \in \mathbb{N}^*$$

Teoremo: $\ell(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_t})$,

$$\ell(1) = 1$$

$$\forall m \geq 2$$

Ex: $m = 10$

$$\ell(10) = 1 \cdot 1, 3, 7, 9 \} = 4$$

$$\ell(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5})$$

Ex: $m=6$ în \mathbb{Z}_6 : $2 \cdot 3 = 6 \equiv 0 \Rightarrow \mathbb{Z}_6$ nu

este inel integral.

Dacă $\exists x, y$ în \mathbb{Z}_m , $\neq 0$ cu $x \cdot y = 0$

atunci \mathbb{Z}_m este INEL INTREGIU
(sau domeniu)

Prop: U.A.S.E (1) \mathbb{Z}_m este domeniu

(2) m este nr. prim

(3) \mathbb{Z}_m este corp (\Leftrightarrow $U(\mathbb{Z}_m)$)

$$= \mathbb{Z}_m \setminus \{0\}$$

\mathbb{Z}_m : $x \equiv y \pmod{m} \Leftrightarrow m|x-y \in \mathbb{Z}$ și $x \equiv y$ sau ocelește
două în \mathbb{Z}_m (e) luate cu restul împ. la m ,
care se rezolvă (căci de) resturi
la împărțirea la m .

Ex: Aflați ultima cifră a lui $x = 32^{30}$.

x poate avea să fie restul împărțirii
 N la 10.

$$N \equiv ? \pmod{10}$$

$$\text{în } \mathbb{Z}_{10}: \widehat{32^{30}} = \widehat{32}^{30} = \widehat{2}^{30} = \widehat{2^3} = \widehat{8}$$

$$32 \equiv 2 \pmod{10}$$

$$\widehat{32} \equiv \widehat{2}$$

$$\begin{aligned} \widehat{2^{30}} &= (\widehat{2^{10}})^3 = \widehat{2^{10}}^3 = \widehat{1024}^3 = \widehat{4^3} = \widehat{64} = \\ &= \widehat{8} \Rightarrow 32^{30} \equiv 8 \pmod{10} \end{aligned}$$

Ierarhia de polinoame A[x]

- „ x ” este un simbol nou, o indeterminata
- Pentru noi $A =$ inel comutativ $\rightarrow \mathbb{Z}$
 L, C, D, Q
 sau \mathbb{Z}_p

Polinom = suma de monome p -prim

Monom = un coefficient multiplu cu un produs de indeterminante din A

$$a \cdot x^n \text{ cu } a \in A$$

gradul monomului x este n .

$$\text{Polinom: } p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

doco $a_n \neq 0$: $LT(p) = a_n x^n$ - termenul dominant al lui p

$$LC(p(x)) = a_n - \text{coefficient dominant}$$

n = gradul polinomului

$\text{grad}(p(x))$ sau $\deg(p(x))$

obs: Pt. polinomul nul $p(x) = 0$, $\deg(0) = -\infty$

$\deg(p(x)) = 0 \Leftrightarrow p(x) = a$ cu $a \in A \setminus \{0\}$

constanta nula

$\text{grad } p(x) = 1 \Leftrightarrow p(x) = ax + b$ cu $a, b \in A$, $x \in A$

not $A[x] = \{a_m x^m + \dots + a_1 x + a_0 \mid m \in \mathbb{N}, a_0, a_1, \dots, a_m \in A\}$

- polinoamele sunt nedeterminante și au coeficienți
din inelul comutativ A .

Teorema $A[x]$ este un inel comutativ cu op. $+^4$

$$(\sum_{i \geq 0} a_i x^i) + (\sum_{i \geq 0} b_i x^i) = \sum_{i \geq 0} (a_i + b_i) x^i$$

$$(\sum_{i \geq 0} (a_i x^i)) \cdot (\sum_{j \geq 0} b_j x^j) = \sum_{i+j=k} (\sum_{i+j=l} a_i b_j) x^k$$

$$\text{Opusul lui } p(x) \text{ este } -p(x) = \sum_{i \geq 0} (-a_i) x^i$$

1 - este elem. neutru la înmulțire

$$A \subseteq A[x]$$

două polinoame coincid \Leftrightarrow au același grad
și același coef.

$$\sum a_i x^i = \sum b_i x^i \Leftrightarrow a_i = b_i \quad \forall i$$

Prop: $\text{grad}(f+g) \leq \max \{\text{grad } f, \text{grad } g\}$
 $\text{grad}(f \cdot g) \leq \text{grad } f + \text{grad } g$

$$f = a_n x^n + \dots \Rightarrow \text{grad } f = n$$

$$\text{grad } f = m, g = b_m x^m$$

$$\text{LT}(f) \cdot \text{LT}(g) = a_n b_m x^{n+m}$$

$$\text{ex: im } \mathbb{Z}_6: 2 \cdot x^5 \cdot 3 \cdot x^8 = 6 \cdot x^{13} = 0$$

"0"

• Dacă $\deg(f) \cdot \deg(g) \neq 0 \Rightarrow \deg(f \cdot g) =$
 $= \deg(f) + \deg(g)$

Mix: dacă $A = \text{corp sau domeniu}$

sau dacă f și g sunt polinoame
monice (sau unitate)

Dif Lm polinom cu coef. dominant = 1 sau
monic

Teorema de împărțire cu rest:

Fie $f, g \in A[x]$ cu $g \neq 0$

Să PP că (A este corp) sau că $\deg(\text{cc}(g))$
este inversabil în inelul A)

Astunci (F!) polinoamele $Q(x), R(x) \in A[x]$

a.t. $f(x) = g(x) \cdot Q(x) + r(x)$; și $\deg r <$
 ↓ ↓ grad g
 cōsul restul

Dem: (Schito) notăm $s(x)$

Ex: Anotăti că în $\mathbb{Z}[x]$ nu putem
împărti cu rest în $f(x) = x^2 + 1$ la
 $g(x) = 2x$